7/9/04

US-PAT-NO: 6587882

DOCUMENT-IDENTIFIER: US 6587882 B1

TITLE: Mobile IP communication scheme using visited site or
nearby network as temporal home network

---------- KWIC ---------

Application Filing Date - AD (1):
19980803

Detailed Description Text - DETX (45):
Note that the **DHCP** supports only communications with respect to subnet, so that in a situation where not necessarily all **DHCP** servers are supporting the function for returning the resource server information, it is difficult to acquire the resource server information from the **DHCP** server by this scheme if the **DHCP** server on the subnet to which the mobile computer 2 moved happened to be not supporting the function for returning the resource server information. In this regard, in a system where the **home agent** of the Mobile IP returns the resource server information, it is possible to use a protocol different from the subnet broadcast, so that there is a flexibility in that it is possible to select a **home agent** that is supporting the function for returning the resource server information by searching through **home agents** on nearby networks rather than using just the **home agent** on the visited site network, even in a situation where not necessarily all **home agents** are supporting the function for returning the resource server information.

Detailed Description Text - DETX (46):
Moreover, when the mobile computer 2 failed to acquire the resource server information from the **DHCP** server of the visited site subnet, for example, it is also possible to activate a program for Mobile IP communication, and acquire the resource server information through the Mobile IP registration processing with respect to a **home agent** on a nearby network, using an address allocated from the **DHCP** server as a Care-of-address and an address leased from the nearby network as a home address.

US-PAT-NO: 6651105

DOCUMENT-IDENTIFIER: US 6651105 B1

TITLE: Method for seamless networking support for mobile devices using serial communications

---------- KWIC ---------

Application Filing Date - AD (1):
19991112

Brief Summary Text - BSTX (12):
A mobile host has a permanent home IP address which does not change upon movement to a new subnet. When a mobile host moves to a new subnet other than its home subnet, it registers its current location--the IP address of a foreign agent in the new subnet or a temporary IP address obtained by mechanisms such as DHCP- with an agent in its home subnet, called home agent. The home agent then intercepts IP packets destined to the mobile device and forwards them to the current location by mechanisms called IP-IP encapsulation and IP tunneling. If the mobile host has registered the IP address of a foreign agent with the home agent, then the packets are forwarded to this foreign agent which then forwards them to the mobile host. If the mobile host has registered a co-located IP address with its home agent, then the packets are directly forwarded to the mobile host. For security reasons, a mobile host authenticates itself to its home agent with each registration. The authentication is based on a shared secret key that can be manually configured in a mobile device and its home agent.

Applicants
cant use

DOCUMENT-IDENTIFIER: US 20020057657 A1

TITLE: PACKET TUNNELING OPTIMIZATION TO WIRELESS DEVICES ACCESSING PACKET-BASED WIRED NETWORKS

---------- KWIC ---------

Application Filing Date - APD (1):
19981211

Brief Description of Drawings Paragraph - DRTX (8):
[0014] FIG. 6 is a block diagram illustrating an exemplary embodiment of a domain router hosting a Dynamic Host Configuration Protocol (**DHCP**) server and a **home agent,** in accordance with the present invention;

Detail Description Paragraph - DETX (27):
[0058] FIG. 6 is an exemplary embodiment of a domain router 260 hosting a Dynamic Host Configuration Protocol (**DHCP**) server 272 and a **home agent** 270. Domain routers are comprised of a plurality of ingress ports (or interfaces) 262 for receiving packets from the previous node and a plurality of egress ports (or interfaces) 264 for sending packets to a next hop. It is also known to those skilled in the art that interfaces may be bidirectional as well. That is, an interface may act as both an ingress and egress interface. Additionally, routers each include a processor 266 and memory 268. The processing and memory resources resident at each router enable the provisioning of router functions and services such as: implementing forwarding algorithms, queuing, signaling, messaging, implementing router forwarding tables, as well as other standard and supplemental router functions and services. The domain router 260 illustrated in FIG. 6 shows a **DHCP** server 272 and **home agent** 270 implemented utilizing the resources of the processor 266 and memory 268. Typically, the domain router 260 in which the **DHCP** server 272 and **home agent** 270 are implemented is the domain root router, but this arrangement is not required by necessity, as previously described. It would be apparent to those skilled in the art to alternatively implement the **home agent and DHCP** server in any local router or node capable of communicating with the other routers (including base stations) within a domain. Furthermore, those skilled in the art would also realize that the **home agent and DHCP** server may be implemented

outside of the router itself using a separate co-located processor and memory, such as that available in a personal computer, with appropriate communications provided with the domain root router. Implementation of a foreign agent within a router, when required, is also performed in like manner.

Detail Description Paragraph - DETX (96):
[0122] Integration of the Routing Information Protocol (RIP) and the Mobile IP standards within a Dynamic Host Configuration Protocol (**DHCP**) server is accomplished in accordance with the following exemplary description. When a mobile device is powered up, it first sends a **DHCP**_DISCOVER message to the base station to which it attaches upon power up. The base station therefore serves as a **DHCP** relay and forwards the **DHCP**_DISCOVER message to the **DHCP** server. The **DHCP** server conveys a reply to the mobile device with a **DHCP**_OFFER message. The mobile device then conveys a **DHCP**_REQUEST message to the base station which relays the message to the **DHCP** server. The **DHCP** server then sends a **DHCP**_RESPONSE, which contains the mobile device's assigned address (the `ciaddr` field), the base station's address (the `giaddr` field), and the domain root router's address (the `siaddr` field). The mobile device then sends an update path setup message to the current base station with a sequence number of zero and with the final destination as the domain root router. This message establishes routing entries in selected routers within the domain so that packets arriving at the domain root router are delivered to the mobile device. When the mobile device is handed off to a new base station within the same domain, it updates its sequence number as previously described and sends a path setup message using the new-to-old path setup scheme to maintain connectivity after handoff. If the mobile device is handed off to a new base station within a new domain, the mobile device acquires a care-of address via the **DHCP** server of the new domain. The mobile device then informs the **home agent** in the previous domain as to its new care-of address. Packets are then tunneled between the **home agent** and the new care-of address for as long as the mobile device is still attached to a base station within the new domain. When the mobile device is powered down, the address assigned from the **DHCP** server in the new domain and/or the address assigned from the **DHCP** server in the original domain are relinquished for reuse.

US-PAT-NO: 6144671

DOCUMENT-IDENTIFIER: US 6144671 A

TITLE: Call redirection methods in a packet based communications network

---------- KWIC ---------

Brief Summary Text - BSTX (6):

The Mobile IP Protocol (defined by the mobile IP work group within the IETF (Internet Engineering Task Force)) is an existing IP (Network) layer procedure for terminal mobility within the Internet/Intranet [Perkins, C., Editor, "IP Mobility Support", RFC 2002, October 1996]. This protocol however, requires the modification of a mobile host's IP stack to handle IP encapsulation or tunnelling, the modification of the home router's IP stack to support the functionalities of a **Home Agent** (i.e. encapsulating/decapsulating and tunnelling both call signalling and media packets to the destination c/o address), the existence of a Foreign Agent on the foreign network (router) to handle IP encapsulation/decapsulation and tunnelling at the far end, procedures to discover and register with **Home Agents** and Foreign Agents, and procedures to gain access to firewalls when the callee's mobile host is attached to a subnetwork behind a firewall.

Detailed Description Text - DETX (81):

When the mobile callee returns home and plugs back his/her MH into the home network 72, the callee's MH sends gratuitous ARP messages 154 (during **bootstrapping**) to bind the callee's home address 120 to the MH's hardware address itself. The callee then deactivates the call redirector 18 on the SH 122 to discontinue the terminal mobility services through the exchange of a deactivation request message 156 and a deactivation reply message 158.

US-PAT-NO: 6055236

DOCUMENT-IDENTIFIER: US 6055236 A

TITLE: Method and system for locating network services with distributed network address translation

---------- KWIC ---------

Detailed Description Text - DETX (27):

In one preferred embodiment of the present invention, a network device transmits a PAP request message 66 upon boot. The PAP 64 is associated with Dynamic Host Configuration Protocol ("DHCP") or **BOOTstrap** Protocol ("BOOTP"). DHCP is a protocol for passing configuration information such as IP 48 addresses to hosts on an IP 48 network. For more information on DHCP see RFC-1541 and RFC-2131, incorporated herein by reference. The format of DHCP messages is based on the format of BOOTP messages described in RFC-951 and RFC-1542, incorporated herein by reference. From a network device's point of view, DHCP is an extension of the BOOTP mechanism.

Detailed Description Text - DETX (152):

The methods for preferred embodiments of the present invention presented herein also extends IPsec within the context of Mobile IP, allowing a mobile node to maintain an IPsec-protected connection while it is roaming. For Mobile IP, a mobile node's **home agent's** global IP address and a mobile nodes local address on its home network can be used for name space binding to create a security certificate to use for IPsec with DNAT. This information is available to a mobile node even while it is roaming (i.e., temporarily residing on a foreign network). A mobile node's home network is managed as a DNAT stub network in which the mobile node resides as a local host when it is not roaming. Using DNAT with Mobile IP is described in co-pending application Ser. No. 09/136,484.

DOCUMENT-IDENTIFIER: US 20020143990 A1

TITLE: MOBILE INTERNET PROTOCOL FOR MOBILITY OF ACCESS HOSTS
BETWEEN NETWORKS

---------- KWIC ---------

Application Filing Date - APD (1):
19981210

Detail Description Paragraph - DETX (6):
[0037] If a mobile host subscribing to the corporate LAN and to the cellular telephone network leaves the coverage area of the corporate LAN and enters that of the cellular telephone network (either GSM or hot spot LAN), the host will deregister with the former whilst registering with the latter. Upon registration with the telephone network, the network assigns and transmits to the mobile host a new internet address in that network. This new address is either one of a number of addresses allocated to the GSM network and defining the **home agent** as the end point, or is dynamically assigned to the mobile host (e.g. using **DHCP**) to define the mobile host as the end point. In either case, the new address replaces the internet address allocated to the host when it was registered to the corporate LAN. Datagrams destined for the mobile host, and initiated via the cellular telephone network, are now sent directly to the cellular telephone network (see reference numeral 4 in FIG. 3). This contrasts with previously proposed roaming protocols where the host retained the internet address assigned by the corporate LAN (i.e. the home network) and used an address assigned by the foreign network only as a care-of-address.

US-PAT-NO: 6535493

DOCUMENT-IDENTIFIER: US 6535493 B1

TITLE: Mobile internet communication protocol

---------- KWIC ---------

Detailed Description Text - DETX (12):

As an alternative for a care-of address, the mobile unit 130 may obtain a co-located care-of address by **BOOTP**/DHCP. The registration occurs between the mobile unit 130 and the home agent. The mobile unit 130 becomes the end of the tunnel and itself performs the decapsulation of the datagrams. Finally, when the mobile unit 130 detects that it has returned to its home subnet, it performs a deregistration process with its home agent.